

# UNITED STATES DISTRICT COURT

for the  
Western District of New York

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Residence located at 8981 Wicklow Manor, Clarence Center,  
New York 14032, and the person of Christopher Grant, for a  
cellphone with call number 716-907-2698

Case No. 18-mj-1054

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York (identify the person or describe property to be searched and give its location): Premises located at 8981 Wicklow Manor, Clarence Center, New York 14032, and the person of Christopher Grant, for a cellphone with call number 716-907-2698, as more fully described in Attachment A, which is attached hereto and incorporated herein by reference.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): Evidence pertaining to violations of violations of Title 18, United States Code, Sections 1343, 1348, and Title 15, United States Code, Sections 78j(b) and 78ff and Title 18, United States Code, Section 2, 371 and 1349, as more fully set forth in Attachment B, which is attached hereto and incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 & 15 U.S.C. § 1343, 1348, 2, 371, 1349-78j(b), 78ff,, and the application is based on these facts: SEE AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of      days (give exact ending date if more than 30 days:     ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

JULIE A. AMATO, SA, Federal Bureau of Investigation  
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/24/18

  
Judge's signature

City and state: Buffalo, New York

JEREMIAH J. MCCARTHY, United States Magistrate Judge  
Printed name and title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Julie A. Amato, being duly sworn, hereby depose and state as follows:

**I. Introduction**

**A. Affiant**

1. I am a Special Agent with the Federal Bureau of Investigation (“Investigating Agency”). As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. During my tenure with the FBI, I have participated in the investigations of numerous frauds, and have conducted physical and electronic surveillance, the execution of search warrants, debriefings of informants, and reviews of taped conversations. Through my training, education, and experience, I have become familiar with the manner in which securities frauds are perpetrated.

2. This Affidavit is made in support of an application for a warrant to search the residence of Christopher Grant (the “Subject Premises”), or alternatively the person of Grant, both described more fully in **Attachment A** hereto, for a cellphone in Grant’s possession with call number 716-907-2698 (the “CG Cellphone”) and for any predecessor cellphone, as described more fully below (collectively, the “Electronic Devices”). This affidavit also seeks authorization to search data stored on the Electronic Devices for the items and information described in **Attachment B** to this Affidavit.

3. This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the warrant, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose report I have read.

**B. The Subject Premises**

4. The Subject Premises is described as a residence located at 8981 Wicklow Manor, Clarence Center, New York 14032. As discussed below, the Subject Premises is believed to be the residence of Christopher Grant. The Subject Premises is a single family residence with gray siding. The Subject Premises is accessible through a door in the front of the house surrounded by white portico. The numbers "8981" appear on the side of the house next to the door. Based on my conversations with other law enforcement agents, I have learned that location information for the CG Cellphone indicates that the CG Cellphone has

routinely been located in or around the Subject Premises. Additionally, based on my training and experience, I know that users of cellphones like the CG Cellphone often keep cellphones on their person when they are inside or outside of their home. Accordingly, this Affidavit also requests authorization to search the person of Christopher Grant. A publicly available image of Grant from Twitter appears below:



### **C. The Subject Offenses**

5. For the reasons detailed below, I believe that there is probable cause to believe that the Electronic Devices contain evidence, fruits, and instrumentalities of violations of the crimes of insider trading, conspiracy to commit insider trading, and aiding and abetting insider trading. These crimes constitute violations of the wire fraud provisions of Title 18, United States Code, Sections 1343 (wire fraud) and 1348 (securities fraud); the securities fraud provisions of Title 15, United States Code, Sections 78j(b) and 78ff, as well as Title 17, Code of Federal Regulations, Section 240.10b-5, which implement those provisions; and aiding and abetting and conspiring to commit these offenses in violation of Title 18, United States Code, Section 2 (aiding and abetting), 371 (conspiracy) and 1349 (conspiracy) (together, the “Subject

Offenses”).<sup>1</sup> As set forth below, there is probable cause to believe that the Electronic Devices are likely to be found at the Subject Premises or on the person of Christopher Grant, and that they are likely to contain evidence of the Subject Offenses.

#### **D. Probable Cause Regarding the Subject Offenses**

##### Overview of the Insider Trading Scheme

6. As described in greater detail below, there is probable cause to believe that Christopher Collins, a New York congressman who sits on the board of directors of Innate Immunotherapeutics Ltd. (“Innate”) and is one of its largest shareholders, acquired material nonpublic information regarding negative trial results for an Innate drug and subsequently disseminated that information to various individuals including his current and former campaign managers and his son. Those individuals then further disseminated the information provided by Collins to friends and family members in certain instances, as described below. Multiple individuals who received this information placed illegal trades in Innate stock, avoiding thousands of dollars of losses when the negative trial results were released.

---

<sup>1</sup> The Title 15 securities fraud statutes cited above make it a crime, among other things, to (1) willfully use a device or scheme to defraud someone or engage in any act, practice, or course of business that operates or would operate as fraud or deceit upon any person; where (2) the defendant’s acts were undertaken in connection with the purchase of securities; (3) the defendant directly or indirectly used an instrumentality of interstate commerce or any facility of any national securities exchange in connection with these acts; and (4) the defendant acted knowingly. Insider trading constitutes a device or scheme to defraud under these statutes where a tipper has a duty to keep material, nonpublic information confidential; and the tipper breaches that duty by trading or by intentionally relaying the information to another with the expectation that the information would be used in connection with securities trading and in exchange for a personal benefit. Title 18, United States Code, Section 1348 has elements akin to Section 1343, except in the context of securities fraud.

Relevant Entities and Persons

7. Based on my review of publicly available information, including social media, and discussions with other law enforcement officers, I have learned the following, in substance and in part:

- a. Innate is an Australian biotechnology company whose shares trade on the Australian Securities Exchange ("ASX"). Innate shares also traded over-the-counter in the United States. Innate's business included the development of a drug called "MIS416," which was meant to treat certain conditions related to multiple sclerosis.
- b. Christopher Collins is a congressman representing the 27th district of New York. Christopher Collins sits on Innate's Board of Directors. Christopher Collins has been a significant shareholder of Innate in the past. As of March 24, 2017, Christopher Collins was Innate's largest shareholder, holding over 37 million shares.
- c. Cameron Collins is Christopher Collins' son. Cameron Collins has been a significant shareholder of Innate in the past. As of March 24, 2017, Cameron Collins held approximately 5.2 million shares (roughly 2.3% of the company's public float) of Innate stock.
- d. Lauren Zarsky, based on social media posts, appears to be Cameron Collins' girlfriend or fiancée. Lauren Zarsky's parents are named Dorothy Zarsky and Stephen Zarsky. Lauren Zarsky also has an uncle named Gene Zarsky.
- e. Christopher Grant is Christopher Collins' former chief of staff.
- f. Michael Hook is Christopher Collins' current chief of staff. Michael Hook is married to Vicki Hook, with whom he has two daughters: Mandi Culhane and Mindy Welninski. Mandi Culhane is married to Michael Culhane, and Mindy Welninski is married to Eric Welninski.
- g. Based on my review of records from phone companies, Apple, and brokerage accounts, and discussions with other law enforcement officers, I believe the following phones to be used by the following individuals:

User	Dial Number	Cellphone
Cameron Collins	716-597-4266	"CC Cellphone"
Lauren Zarsky	908-279-4672	"LZ Cellphone"
Dorothy Zarsky	201-715-1474	"DZ Cellphone"
Stephen Zarsky	908-803-3645	"SZ Cellphone"
Michael J. Hook	202-236-9044	"MH Cellphone"
Christopher Grant	716-907-2698	"CG Cellphone"
Michael John Culhane	412-953-7313	"MC Cellphone"
Eric Joseph Welninski	716-830-8529	"EW Cellphone"

### Innate Drug Trial Results

8. Based on my conversations with other law enforcement agents who have reviewed notes from conversations with representatives of the SEC, publicly available information, and other records, I have learned the following, in substance and in part:

- a. On or about Thursday, June 22, 2017 in the United States (which was Friday, June 23, 2017 in Sydney, Australia), Innate filed a press release stating, in substance and in part, that the results of a trial of MIS416 would be announced shortly and that trading in Innate stock on the ASX would be halted "until the earlier of the commencement of normal trading on Tuesday, 27 June 2017 or when the announcement is released to the market" (the "Halt Request"). Based on my training and experience, I know that trading halts are sometimes requested in foreign markets in advance of significant announcements and are not indicative of whether the announcement will be positive or negative.
- b. Although trading in Innate stock was subsequently halted on the ASX, Innate's stock continued to be traded over-the-counter in the United States without restriction.
- c. On or about Monday, June 26, 2017 in the United States (which was Tuesday, June 27, 2017 in Sydney, Australia), Innate announced the results of a clinical trial showing that MIS416 "did not show clinically meaningful or statistically significant differences" over a placebo on various important metrics (the "MIS416 Announcement"). Within days of the MIS416 Announcement, the trading price of Innate's stock fell by over 90%. Prior to the MIS416 Announcement, there had been little public reason to believe that MIS416 would fail the trial. To the contrary, on or about Tuesday, June 20, 2017 in the United States (which was Wednesday, June 21, 2017 in Sydney, Australia), Innate had announced

that the U.S. Food and Drug Administration had cleared MIS416 for additional clinical trials in the United States (the “FDA Announcement”). A press release issued by Innate on the same day described this clearance as “a further important milestone in the ongoing clinical development of the Company’s lead drug candidate MIS416.”<sup>2</sup>

Trading on Advance Knowledge of Innate Drug Trial Results

9. Based on my conversations with other law enforcement agents who have reviewed notes from conversations with representatives of the SEC, publicly available information, and other records, I have learned the following, in substance and in part:

- a. As discussed, Christopher Collins was one of Innate’s largest shareholders and a member of its board of directors. Based on my training and experience, I know that individuals who are members of a company’s board of directors commonly receive material nonpublic information in advance of that information being publicly released.
- b. Although Christopher Collins does not appear to have purchased or sold Innate stock in the days immediately preceding the MIS416 Announcement,<sup>3</sup> there is probable cause to believe that Christopher Collins learned of the MIS416 Announcement before it was made public and provided advance information of the MIS416 Announcement to certain family members and close associates, who in turn passed that information onto others for the purpose of trading on it, including the following:
  - i. Cameron Collins. As of June 9, 2017, Cameron Collins owned over approximately 5.2 million shares of Innate stock held in two separate trading accounts (the “Cameron Collins Accounts”). On or about June 23, 2017, after the Halt Request but before the MIS416 Announcement, over approximately 50 sale orders were placed through the Cameron Collins Accounts, resulting in the sale of approximately 616,508 shares of Innate stock in the United States. On or about June 26, 2017, still before the MIS416 Announcement, moreover, orders

---

<sup>2</sup> Innate’s stock does not appear to have appreciated as a result of this announcement.

<sup>3</sup> According to media reports, Collins lost millions of dollars as a result of the decline in Innate’s share price following the MIS416 Announcement. *See, e.g.,* Doni Bloomfield & Brandon Kochkodin, *GOP Lawmaker Loses \$17 Million After Favorite Pharma Stock Plunges*, Bloomberg (June 27, 2017), available at <https://www.bloomberg.com/news/articles/2017-06-27/gop-lawmaker-loses-17-million-as-favorite-pharma-stock-plunges> (last accessed Sept. 22, 2017).



were placed through one of the Cameron Collins Accounts to sell an additional 775,000 shares of Innate in the same manner, for a total of 1,391,500 shares. These sales allowed Cameron Collins to avoid approximately \$571,000 in losses. Additionally, as discussed below, Cameron Collins' girlfriend or fiancée Lauren Zarsky, her parents, and her uncle sold Innate stock immediately before the MIS416 Announcement and therefore avoided significant losses.

ii. Lauren Zarsky. On or about June 19, 2017, a brokerage account was opened in Lauren Zarsky's name (the "Lauren Zarsky Account"). On or about the same day, the Lauren Zarsky Account was wired approximately \$23,000 from a bank located in New York, New York. As discussed below, the Lauren Zarsky Account both purchased Innate shares immediately before the positive FDA Announcement, and then sold Innate shares immediately before the negative MIS416 Announcement.

- On or about June 19, 2017, an order was placed through the Lauren Zarsky Account to purchase over approximately 20,000 shares of Innate stock. This order was placed using an internet connection associated with Cameron Collins's home address. The next morning, on or about June 20, 2017, the Lauren Zarsky Account was used to purchase additional shares of Innate stock, for a combined total of approximately 40,464 shares. Notably, these purchases occurred shortly before the FDA Announcement, which occurred on or about the night of Tuesday, June 20, 2017.
- On or about June 23, 2017, after the Halt Request but before the MIS416 Announcement, a limit order was placed through the Lauren Zarsky Account that resulted in the sale of all Innate shares in that account. Through these sales, the account avoided losses of approximately \$19,400.

iii. Dorothy Zarsky. As discussed above, Dorothy Zarsky is Lauren Zarsky's mother and is married to Stephen Zarsky. From on or about September 14, 2016 through on or about June 22, 2017, approximately 50,000 shares in Innate stock had been consistently held in a brokerage account in Dorothy Zarsky's name (the "Dorothy Zarsky Account"). On or about June 22, 2017, the day of the Halt Request but prior to the Halt Request being made public, a limit order was placed through the Dorothy Zarsky Account that contemplated the sale of approximately all 50,000 shares on the ASX. Because of the price specified in the limit order, only about half of the shares were sold before the trading

halt went into effect. On or about June 23, 2017, after the Halt Request but before the MIS416 Announcement, a limit order was placed to sell the remaining shares in the Dorothy Zarsky Account on United States over-the-counter markets. This limit order was set below the trading price, and was filled. The combined effect of these sales allowed Dorothy Zarsky to avoid approximately \$22,700 in losses that would have accrued had she sold her stock after the MIS416 Announcement.

- iv. Stephen Zarsky. As of on or about May 31, 2017, an IRA account in Stephen Zarsky's name (the "Stephen Zarsky Account") held approximately 303,005 shares of Innate stock. On or about June 23, 2017, after the Halt Request but before the MIS416 Announcement, a limit order was placed through the Stephen Zarsky Account directing the sale all Innate shares at a price below the previous day's closing price. The order was executed as soon as U.S. over-the-counter markets opened. These sales allowed Stephen Zarsky to avoid losses of approximately \$144,000.
- v. Gene Zarsky. As of on or about May 31, 2017, a brokerage account in Gene Zarsky's name held approximately 9,000 shares of Innate stock. On or about June 23, 2017, after the Halt Request and before the MIS416 Announcement, an order was placed to sell all 9,000 shares of Innate stock in the Gene Zarsky Account. By selling prior to the MIS416 Announcement, Gene Zarsky avoided losses of approximately \$4,300.
- vi. Christopher Grant. As discussed above, Christopher Grant is Christopher Collins' former chief of staff. On or about May 31, 2017, brokerage accounts in Grant's name (the "Grant Brokerage Accounts") held approximately 23,300 shares of Innate stock. On or about June 23, 2017, after the Halt Request but before the MIS416 Announcement, all of the Innate stock in the Grant Brokerage Accounts was sold in the United States. These sales allowed Grant to avoid losses of approximately \$11,200.
- vii. Michael Hook. As discussed above, Michael Hook is Christopher Collins' current chief of staff. Michael Hook is married to Vicki Hook.<sup>4</sup> Although the Government has not to date identified

---

<sup>4</sup> See, e.g., Nate Hoffman, *Rep. Collins keeps it all in the family*, Legistorm (Oct. 2, 2015) ("The congressman's new chief of staff, Mike Hook, is the uncle of the congressman's legislative assistant. . . . The 56-year old has come on board to replace Christopher Grant, who took a job with Axiom Strategies while being investigated as part of a state corruption case. . . . Mike's wife, Vicki, also made a name for herself on Capitol Hill. She was the chief of staff for former Rep. Vito Fossella (R-N.Y.) and the deputy chief of staff for Rep. Tom Reed (R-N.Y.).") (last accessed Sept. 22, 2017). Further, a Facebook account in the name of Vicki Hook is "friends" with accounts in the names of "Michael Hook," "Mandi Scott Culhane," "Michael Culhane," and "Mindy Scott."

trading by Hook prior to the MIS416 Announcement, individuals who appear to be Hook's family members sold shares in Innate during this period:

- Public records indicate that Mandi Culhane previously shared an address with Vicki Hook. As of on or about May 31, 2017, Mandi Culhane and Michael Culhane, who is believed to be her husband, held approximately 201,000 shares of Innate stock in two separate brokerage accounts. On or about June 23, 2017, after the Halt Request but before the MIS416 Announcement, orders were placed to sell all Innate shares in both accounts in U.S. over-the-counter markets. The sales allowed the Culhanes to avoid losses of approximately \$83,600.
- Public records indicate that Mindy Welninski previously shared an address with Vicki Hook and is currently married to Eric Welninski. As of on or about May 31, 2017, Eric Welninski held approximately 110,700 shares of Innate stock in a single account. On or about June 23, 2017, after the Halt Request but before the MIS416 Announcement, an order was placed to sell all Innate shares in that account in U.S. over-the-counter markets. This sale allowed Eric Welninski to avoid losses of approximately \$47,700.

10. Based on my training and experience, I believe that the above-referenced trading patterns are consistent with the dissemination of material nonpublic information regarding the MIS416 Announcement from Christopher Collins to his son; from Christopher Collins to his former chief of staff, Christopher Grant, who then traded on the information; and from Christopher Collins to his chief of staff, Michael Hook, who then disseminated the information to certain of his family members.

Dissemination of Material Nonpublic Information  
Regarding the Failed MIS416 Trial to Christopher Collins

11. Law enforcement agents have reviewed emails sent from an email account used by Gary Cutter, who was in communication with Simon Wilkinson, Innate's CEO, regarding

the results of the MIS416 trial. Cutter is a professor at University of Alabama at Birmingham who, according to the university's website, specializes in biostatistics. These emails include an email chain between Cutter, Wilkinson, and Michael Silverman, who acted as a consultant to Innate during the clinical trials of MIS416. The email chain appears to begin at 6:01 PM EDT on June 22, 2017, with Silverman forwarding Wilkinson a previously composed email with subject line "Innate data." It appears that attached to that email were two files, titled "Top-line for Simon 23 June 2017.zip" and "Innate Top-Line Summary Final PW.xlsx." A string of emails then followed between Cutter, Silverman, and Wilkinson.

12. From the e-mail chain, it appears that on June 22, 2017, at 6:58 PM EDT, Wilkinson sent the following email to Cutter and Silverman:

Hi Guys

Thanks for your careful analysis and report.  
I have just sent the unfortunate news on to the board and no doubt as things sink in there will be some questions.

Would either or both of you potentially be available to come onto a call if requested to answer any initial questions – depending on the time of day of course!

Sincere thanks – Simon

Based on this email, there is probable cause to believe that Christopher Collins, who, as discussed above, was a member of Innate's Board, received advance notice of the MIS416 Announcement at some point before June 22, 2017 at 6:58 PM EDT, when Wilkinson stated that he had already "sent the unfortunate news on to the board."

Communications with and Trading by Cameron Collins

13. Phone records obtained from AT&T Wireless indicate that at 7:16 PM EDT on June 22, 2017, the user of a cellphone known to be used by Christopher Collins placed a call to the CC Cellphone that lasted approximately six minutes.

14. Brokerage records indicate that at approximately 7:38 PM EDT on June 22, 2017, Lauren Zarsky's brokerage account was accessed from an IP address associated with AT&T Wireless. The CC Cellphone and the LZ Cellphone are both serviced by AT&T Wireless. Although there does not appear to be a data packet that corresponds to the 7:38 PM EDT account log-in on Records relating to the LZ Cellphone, there does appear to be a data packet corresponding to that time on the records for the CC Cellphone.

15. Location information maintained by the service providers for the CC Cellphone and the LZ Cellphone indicate that between 7:16 PM and 7:38 PM EDT on June 22, 2017 both cellphones were using the same tower in the vicinity of an apartment located at 44 Prospect Street, Morristown, NJ 07960 ("the Cameron Collins Residence"), which is listed in brokerage records as the residence of Cameron Collins. Moreover, data records for the LZ Cellphone and the CC Cellphone indicate that from 7:30 PM to 8:55 PM EDT on June 22, 2017 both phones were accessing the internet in the vicinity of Cameron Collins Residence. After 8:55 PM EDT, both phones began heading southeast, eventually coming to rest in the vicinity of a residence located at 28 Club Lane in Summit, New Jersey, 07901 (the "Zarsky Residence"), which is listed in brokerage records as the residence of both Dorothy and Stephen Zarsky.

16. At approximately 9:02 PM EDT on June 22, 2017, Lauren Zarsky's brokerage account was accessed from an IP address registered to AT&T Wireless. Records from the LZ Cellphone indicate that the phone was accessing the internet at that time.

17. At approximately 9:22 PM EDT on June 22, 2017, Cameron Collins's brokerage account was accessed from an IP address registered to Dorothy Zarsky at the Zarsky Residence (the "Dorothy Zarsky IP"). At approximately 9:28 PM EDT, Dorothy Zarsky's brokerage account was accessed from the same IP address.

18. At 9:34 PM EDT on June 22, 2017, Dorothy Zarsky used the DZ Cellphone to place a call to her brokerage firm. During the course of the call, which lasted over 20 minutes, Zarsky placed the above-referenced limit order that contemplated the sale of 50,000 shares of Innate stock (all of her holdings) on the ASX, using a computer logged in from the IP address registered at the Zarsky Residence.

19. At 10:53 PM EDT on June 22, 2017, the trading halt in Innate was announced on the Bloomberg News Service. At 11:57 PM EDT, the CC Cellphone was in communication with the Christopher Collins's Cellphone for approximately one minute and thirty seconds. Shortly thereafter, at approximately 12:01 AM EDT on June 23, 2017, the user of the LZ Cellphone contacted the user of the SZ Cellphone, and they spoke for approximately five minutes.

20. On the morning of the June 23, 2017, at 7:34 AM EDT, Cameron Collins's brokerage account was accessed from the Cameron Collins Residence. An order to sell over approximately 16,000 shares of Innate was placed at approximately 7:42 AM EDT. At about the same time, a call was placed from the LZ Cellphone to the SZ Cellphone. The call lasted for just over four minutes. Shortly thereafter, at 7:52 AM EDT, Stephen Zarsky placed an order to sell over 300,000 shares of Innate. Additionally, Lauren Zarsky placed an order to sell her holdings in Innate at approximately 9:37 AM EDT.

21. After Stephen Zarsky sold his holdings in Innate, at 9:40 AM EDT the SZ Cellphone was in communication with a cellphone used by Gene Zarsky. At 9:43 AM EDT, Gene Zarsky placed an order to sell his holdings in Innate.

22. Based on my training, experience and participation in this investigation, I believe that the above-referenced pattern of trades and communications suggests that Cameron Collins, Lauren Zarsky and Stephen Zarsky may have used the trading halt as a pretext to trade on inside information regarding the MIS416 results that they obtained from Christopher Collins. Additionally, as set forth below, the communications between Hook and his sons-in-law indicate a similar effort.

Communications with and Trading by Michael Culhane and Eric Welinski

23. Location information for Christopher Collins and Michael Hook indicate that both men were in the vicinity of the federal capital building in Washington, DC at

approximately 6:57 PM EDT on June 22, 2017, the time at which it appears, based on the email chain above, Innate's CEO informed Innate's Board of the negative test results.

24. On the morning of June 23, 2017, at 7:18 AM EDT, Michael Hook forwarded an email chain to Michael Culhane, Eric Welninski, Mandi Culhane, and Mindy Welninski<sup>5</sup> indicating that a trading halt had been announced in Innate. Hook commented on the news, advising that "[a] halt in trading means the company is likely to have bad news." In the earlier email that Hook had forwarded, Hook also stated, "[a] trading halt means bad news."

25. Despite this advice, Michael Hook himself, who had substantial holdings in Innate, did not sell his Innate stock in the gap between the Halt Request and the MIS416 Announcement. Moreover, as discussed, trading halts are not necessarily indicative of bad news and Innate itself had previously been halted on at least one occasion earlier in 2017. Based on these facts, and the proximity of Michael Hook to Christopher Collins at the time Collins apparently learned the bad news regarding the MIS416 trial, there is probable cause to believe that Michael Hook knew that the results of the trial were negative at the time he sent the above-quoted email, in which he advised that a trading halt indicated bad news.

26. Indeed, there is probable cause to believe that, despite failing to sell his own Innate shares, Hook caused others to do so. For example:

---

<sup>5</sup> The names on the email appear as "Mandi Scott" and Mindy Scott." I understand "Scott" to be both individuals' middle name (their last names are, respectively, Culhane and Welninski). I know that the appearance of the names in the email may be a result of how the names are entered electronically in contact books or by the users of the account.



- a. Toll records indicate that at approximately 7:49 AM EDT on June 23, 2017, the MH Cellphone called the CG Cellphone, and a conversation of over 17 minutes ensued. Shortly thereafter, at approximately 8:28 AM EDT, Grant logged into his brokerage account from an IP address associated with AT&T Wireless, the provider of his cellphone service, and sold substantially all of his holdings in Innate.
- b. Archived iMessages obtained through a search of Michael Hook's iCloud account show that on June 23, 2017, Hook encouraged Michael Culhane to sell his holdings in Innate:

Time	Sender	Recipient	Content
11:02 AM EDT	Hook	Culhane	You should call Eric and tell him what you're doing.
11:03 AM EDT	Culhane	Hook	I'll do that. I'm just watching it for now. Up to about 800k in volume and .48 a share.
11:19 AM EDT	Hook	Culhane	Just told Eric that I consider a halt bad news.
3:52 PM EDT	Culhane	Hook	I was able to sell all OTC. Made some profit and have no risk now. Just wanted to let you know.

- c. Consistent with the indications above, the EW Cellphone and the MC Cellphone were in direct communication with each other during the relevant period. Specifically, at 11:03 AM EDT on June 23, 2017, the MC Cellphone was used to call the EW Cellphone. The parties spoke for approximately nine minutes. At 12:10 PM EDT, the EW Cellphone was in contact with the MC Cellphone for approximately one minute. Additionally, phone records reflect that, between approximately 2:01 PM EDT and 2:04 PM EDT, the EW Cellphone and the MC Cellphone exchanged a series of text messages that the Government has not been able to obtain by searching their respective iCloud accounts.

Probable Cause to Believe that Christopher Grant Resides in the Subject Premises

27. Based on my conversations with other law enforcement agents, I understand that brokerage records and cellphone billing records list the Subject Premises as Christopher Grant's address. Further, based on my review of data collected in response to a tracking warrant signed on or about March 2, 2018, I have learned that the CG Cellphone is consistently located in the vicinity of the Subject Premises.

Probable Cause to Believe that the Subject  
Premises Contain Evidence of the Subject Offenses

28. For the reasons described above, there is probable cause to believe that the CG Cellphone will contain evidence of the insider trading scheme described herein. As discussed above, the CG Cellphone was in contact with Michael Hook shortly before Grant, the user of the CG Cellphone, sold shares of Innate. It is also likely that the CG Cellphone contains other evidence of the insider trading scheme. Based on my training and experience, for example, I know that iMessages, which are transmitted over the internet, are not captured by toll records. And while they may sometimes be backed up by the user and saved on servers maintained by Apple, this is not always the case and depends on actions by the user. Consequently, without searching the physical devices, the Government is unable to determine whether certain individuals exchanged iMessages during the relevant period.

29. I also know, based upon my training and experience that individuals who engage in insider trading schemes commonly store records and communications relating to their illegal activity on cellphones. Such records can include, for example, text and voice messages; logs of online "chats" with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts; and records of illegal transactions including trading records, bank records and other financial records. Individuals engaged in criminal activity often store such records in order to, among other things, keep track of co-conspirator's contact information; keep a record of illegal transactions for future reference; keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds

with co-conspirators; and store stolen data for future exploitation. Such individuals often fail to delete relevant records such as communications relating to their scheme.

30. In addition, the majority of the trading activity that is the subject of this investigation was conducted online and so accordingly could have been effected through the use a smartphone like the CG Cellphone. Based on my training and experience I know that searches of cellphones may yield evidence that at or near the time a trade was placed or a brokerage account was accessed, a particular individual logged into his or her email, conducted a distinctive web search, or took some other action with the computer or phone that would allow investigators to identify who was operating the device at the time of the suspicious trade.

31. Based on my training and experience, I also know that, where electronic devices are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Even when a user updates or replaces a smart phone, it is often the case that some or all of the contents of the old phone are transferred to the new phone, including any historical message, call detail and browsing history.
- Electronic files can be stored on a hard drive for years at little or no cost, and users thus have little incentive to delete data that may be useful to consult in the future.
- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more

recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.

32. In addition to authorization to seize and search for the specific cellphone identified above, this Affidavit also seeks authorization to search a predecessor cellphone that may have been in use at the time the Subject Offenses occurred. I know, based on information obtained from Grant's cellphone carrier, that at the time of the June 2017 communications set forth above, Grant used an Apple iPhone Model 6S, with International Mobile Equipment Identity ("IMEI") number 35329507462078, serviced by AT&T, and with call number (716) 907-2698. I also know, based on my training and experience, that individuals generally replace or update cellphones with some regularity. When doing so, individuals will oftentimes keep old cellphones for various reasons, including for use as a backup or because the phone contains stored data. To the extent an Apple iPhone Model 6S, with IMEI number 35329507462078, is also available in the Subject Premises, that cellphone may accordingly retain evidence of the Subject Offenses.

33. Based on the foregoing, I respectfully submit there is probable cause to believe that the Electronic Devices contains evidence of the Subject Offenses, including:

- Evidence concerning trades placed in Innate Immunotherapeutics Ltd., including communications regarding the same;
- Communications regarding Innate Immunotherapeutics Ltd.;
- Evidence concerning the location of the user of the device and the times the device was used;

- Evidence concerning the identity or location of, and communications with, coconspirators, including, but not limited to, photographs, contact lists, address books;
- Evidence concerning any proceeds or benefits received as a result of the commission of the Subject Offenses.

In addition to probable cause to believe that the Electronic Devices contain evidence of the Subject Offenses, there is also probable cause to believe that the Electronic Devices also constitute an instrumentality of the Target Offenses because they were used in relation to the insider trading scheme described above.

34. Moreover, for the reasons set forth above, and based on cellphone location information, I submit that there is probable cause to believe that the CG Cellphone will be found in the Subject Premises or on Grant's person.<sup>6</sup>

## **II. Procedures for Searching ESI**

### **A. Execution of Warrant for ESI**

35. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with Rule 41, this application requests authorization to seize the Electronic Devices found in the Subject Premises and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

---

<sup>6</sup> Law enforcement agents also intend to execute the searches described in this Affidavit in the early morning, at a time when the relevant individuals (and their phones) are likely to be physically located in the Subject Premises.

- First, the volume of data on cellular phones is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because electronic data is particularly vulnerable to inadvertent or intentional modification or destruction, such devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of cellular phones and cellular phone operating systems in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying data.
- Fourth, many factors can complicate and prolong recovery of data from a cellular phone, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the phone, which often take considerable time and resources for forensic personnel to detect and resolve.

#### **B. Accessing ESI**

36. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, the following:

- a. Some models of smartphones such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. For iPhones, this feature is called Touch ID. I also know that the Apple iPhone X offer its users the ability to unlock the device via the use of facial recognition (through infrared and visible light scans) in lieu of a numeric or alphanumeric passcode or password. This feature is called Face ID.
- b. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device. If a user enables Face ID on a given Apple device, he or she can unlock the device by raising the iPhone to his or her face, or tapping the screen. In my training and experience,

users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents.

- c. In some circumstances, Touch ID or Face ID cannot be used to unlock a device that has either security feature enabled, and a passcode or password must be used instead. These circumstances include: (1) when the device has just been turned on or restarted; (2) when more than 48 hours has passed since the last time the device was unlocked; (3) when the passcode or password has not been entered in the last 6 days, and the device has not been unlocked via Touch ID in the last 8 hours or the device has not been unlocked via Face ID in the last 4 hours; (4) the device has received a remote lock command; or (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made.
- d. The passcodes or passwords that would unlock the Electronic Devices are not known to law enforcement. Thus, it will likely be necessary to press the fingers of the user of the Electronic Devices to the device's Touch ID sensor, or hold the relevant device in front of the user's face to activate the Face ID sensor, in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple devices via Touch ID with the use of the fingerprints of the users, or via Face ID by holding the device in front of the users' faces, is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.
- e. Based on these facts and my training and experience, it is likely that Grant is the user of the CG Cellphone and any predecessor phones, and thus that his fingerprints are among those that are able to unlock the devices via Touch ID, or his face is able to unlock the devices via Face ID. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Electronic Devices as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.
- f. I also know from my training and experience, and my review of publicly available materials published by Apple that Apple brand devices have a feature that allows a user to erase the contents of the device remotely. By logging into the Internet, the user or any other individual who possesses

the user's account information can take steps to completely wipe the contents of the device, thereby destroying evidence of criminal conduct, along with any other information on the device. The only means to prevent this action is to disable the device's ability to connect to the Internet immediately upon seizure, which requires either access to the device itself to alter the settings, or the use of specialized equipment that is not consistently available to law enforcement agents at every arrest.

- g. At the time the agents execute the requested warrant, they will ask Grant for the passcode or password for any seized devices. If he refuses to provide the password or passcode, I request that the Court authorize law enforcement to press the fingers (including thumbs) of Grant to the Touch ID sensor of the seized device, or hold the seized device in front of Grant's face, for the purpose of attempting to unlock the device via Touch ID or Face ID in order to search the contents as authorized by this warrant.

### **C. Review of ESI**

37. Following seizure of any electronic devices and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

38. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);



- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation<sup>7</sup>; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the electronic device was used.

39. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices to evaluate its contents and to locate all data responsive to the warrant.

#### **D. Return of ESI**

40. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Electronic data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

---

<sup>7</sup> Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

### **III. Conclusion and Ancillary Provisions**

41. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in **Attachment B** to this affidavit and to the Search and Seizure Warrant.

42. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise. Although Grant will know that the search was executed when it occurs, unsealing this affidavit and the associated papers would allow Grant to learn about the Government's investigation, including its ongoing investigation of multiple other people involved in the Subject Offenses. This risks destruction of evidence and hindering the Government's investigation. Disclosing details regarding the Government's investigation would facilitate the destruction of evidence and collusion among the subjects of the Government's investigation, who would know what and whom exactly the Government was investigating, how so, and the Government's particular theories. To the extent the Government were to interview the subjects or subpoena their testimony, such steps would be less effective if this affidavit and related materials were unsealed. Further, disclosure would enable the subjects of the Government's investigation to determine which forms of

communications have been the subject of process, such emails and iMessages, and discontinue those methods.



Julie A. Amato, Special Agent  
Federal Bureau of Investigation

Sworn to before me this 24<sup>th</sup> day  
of April, 2018.



HON. JEREMIAH J. McCARTHY  
United States Magistrate Judge

**Attachment A**

**Property and Person to be Searched**

The premises to be searched (the "Subject Premises") is located at 8981 Wicklow Manor, Clarence Center, New York 14032. The Subject Premises is a single family residence with gray siding. The Subject Premises is accessible through a door in the front of the house surrounded by white portico. The numbers "8981" appear on the side of the house next to the door.

The person to be searched is Christopher Grant, as pictured below:



**Attachment B**

**Items to be Searched and Seized**

**A. Evidence and Instrumentalities of the Subject Offenses**

1. Law enforcement personnel are authorized to seize a cellphone in Grant's possession with call number 716-907-2698 and any predecessor Apple iPhone Model 6S, with International Mobile Equipment Identity ("IMEI") number 35329507462078 (the "Electronic Devices"), and, during the execution of this search warrant, are authorized to depress the fingerprints and/or thumbprints of Christopher Grant onto the Touch ID sensor of the cellphones, or hold the cellphones in front of Grant's face to activate the Face ID sensor, in order to gain access to the contents of any such device as authorized by this warrant.

2. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review and seize the ESI contained on the Electronic Devices for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), 1348 (securities fraud), and Title 15, United States Code, Sections 78j(b) and 78ff, as well as Title 17, Code of Federal Regulations, Section 240.10b-5 (securities fraud), and aiding and abetting and conspiring to commit these offenses in violation of Title 18, United States Code, Section 2 (aiding and abetting), 371 (conspiracy) and 1349 (conspiracy) (the "Subject Offenses") described as follows:

- a. Evidence concerning trades placed in Innate Immunotherapeutics Ltd., including communications regarding the same;
- b. Communications regarding Innate Immunotherapeutics Ltd.;
- c. Evidence concerning the location of the user of the device and the times the device was used;
- d. Evidence concerning the identity or location of, and communications with, coconspirators, including, but not limited to, photographs, contact lists, address books;
- e. Evidence concerning any proceeds or benefits received as a result of the commission of the Subject Offenses.

## **B. Review of ESI**

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (which may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.